[Insert Cover Picture]

National Monuments and Icons Tabletop Exercise

Situation Manual

[Date]

Photo Courtesy of [insert source]

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

Exercise Agenda

Start Time	End Time	Activity
8:15 a.m.	9:00 a.m.	Registration
9:00 a.m.	9:15 a.m.	Welcome and Participant Briefing
9:15 a.m.	10:15 a.m.	Module One: Intelligence and Information Sharing
10:15 a.m.	10:30 a.m.	Break
10:30 a.m.	11:30 a.m.	Module Two: Incident Response
11:30 a.m.	12:00 p.m.	Break
12:00 p.m.	1:00 p.m.	Module Three: Short-Term Recovery
1:00 p.m.	1:30 p.m.	Hot Wash
**All times are approximate*		

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	National Monuments and Icons Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [exercise duration] at [exercise location]. Exercise play is limited to [exercise parameters]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [adjust as necessary to reflect exercise objectives]
Capabilities	• Economic Recovery • Environmental Response / Health and Safety • Fatality Management Services • Health and Social Services • Intelligence and Information Sharing • On-Scene Security, Protection, and Law Enforcement • Operational Communications • Operational Coordination • Planning • Public Health, Healthcare, and Emergency Medical Services (EMS) • Public Information and Warning • Situational Assessment • [Additional capabilities as identified]

Objectives	1. Examine pre-incident intelligence and information sharing procedures in relation to a credible threat to domestic critical infrastructure between public and private stakeholders. 2. Examine private sector stakeholders' emergency preparedness plans and response to procedures to a threat-initiated incident and coordination activities with local, state, and federal agencies. 3. Examine short-term recovery plans and business continuity plans following an attack. 4. [Additional objectives as identified]
Threat or Hazard	Improvised Explosive Device (IED)
Scenario	An interactive, discussion-based exercise focused on an IED attack. The scenario consists of three modules: Intelligence and Information Sharing, Incident Response, and Short-Term Recovery.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being used, if applicable]
Participating Organizations	[Please see Appendix A.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).]

General Information

Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes from the TTX. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

Exercise Objectives	Capability
Examine pre-incident intelligence and information sharing procedures in relation to a credible threat to domestic critical infrastructure between public and private stakeholders	✓ Intelligence and Information Sharing ✓ Public Information and Warning
Examine private sector stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and coordination activities with local, state, and federal agencies.	✓ Environmental Response / Health and Safety ✓ Fatality Management Services ✓ On-Scene Security, Protection, and Law Enforcement ✓ Operational Communications ✓ Operational Coordination ✓ Planning ✓ Public Health, Healthcare, and EMS ✓ Situational Assessment
Examine short-term recovery plans and business continuity plans following an attack.	✓ Economic Recovery ✓ Fatality Management Services ✓ Health and Social Services ✓ Operational Coordination
[Insert additional objectives as necessary]	✓ [Insert additional capabilities as necessary].

Table 1. Exercise Objectives and Associated Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Observers do not directly participate in the exercise; however, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitator:** The facilitator provides situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
- **Evaluators:** Evaluators are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Intelligence and Information Sharing
- Module Two: Incident Response
- Module Three: Short-Term Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [mission area] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your jurisdiction's / organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.

- Issue identification is not as valuable as suggestions and recommended actions that could improve [mission area] efforts. Problem-solving efforts should be the focus.
- The assumption is the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

Module One: Intelligence and Information Sharing

Scenario

[Insert Location]

[Month, Day, Year]: [Time]

An international terrorist organization, tired of U.S. foreign policy, has been sharing blog posts indicating they intend to attack important American national monuments to send a message to the United States government. They attest that attacking these locations will not only cause casualties, but will also damage the historical icons, which will provoke and offend the American government and people. Furthermore, an attack on any of these monuments will damage American resolve, as the monuments represent the nation's history.

The organization posts the times of year the monuments experience the highest tourist visits, the facilities at each monument, and basic security observations. Some of the more recent posts have provided various site measurements, including how close vehicle traffic can get to the monuments, and how many security personnel are onsite. The most recent post provided a list of monuments that have metal detectors and security checkpoints for visitors.

As the posts become more specific, the Secretary of Homeland Security, in coordination with other federal entities, issues an "Elevated" Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible terrorist threat against the United States. At this time, there is no specific information that would warrant the release of an "Imminent" Threat Alert. The alert indicates the international terrorist organization is using IEDs and is focused on national icons around the United States. The alert is to remain in place for [amount of time], ending on [date].

The alert gave no specificity about a location at this time. Receiving word about the heightened threat environment, the [insert fusion center] alerts the [local jurisdiction], warning them of potential attacks in and around [insert national monument].

Discussion Questions

1. How would your organization expect to receive information regarding the credible threat?
2. What local, state, federal, or external organization(s) provide this information?

   a. Does your organization have established working relationships with these organizations and rapid means of contacting them?

3. What role does the fusion center have in sharing information with your organization?
   a. Does your organization communicate with the fusion center on a regular basis?
4. Does your organization currently use the Homeland Security Information Network (HSIN) portal?
5. With credible threat information linked to the targeting of national monuments and icons, how do federal intelligence agencies (i.e., Department of Homeland Security [DHS] Office of Intelligence and Analysis, Federal Bureau of Investigation [FBI], National Operation Center) share information with other federal entities?
6. What technology platforms does your organization use to officially share information about the credible threat, potential protective measures, or the status of possible investigations?
7. Should your organization share information with a private sector stakeholder related to potential threats against its location and personnel?
   a. If so, who should receive this information?
   b. How would your organization communicate that information?
8. For private sector stakeholders, what internal information sharing and dissemination process does your organization currently use?
9. What process does your organization use to share information with locations in other states or regions across the National Monuments and Icons subsector?
   a. What about across the Government Facilities Sector as a whole?
   b. Who are the key stakeholders or organization with whom your organization must communicate to protect your critical infrastructure assets?
10. Would your organization share this information with international partners?
11. Are there technological barriers, policies, legal considerations, or institutional sensitivities that might affect information sharing?

MODULE TWO: INCIDENT RESPONSE

Scenario

[Insert Location]

[Month, Day, Year]: 12:40 p.m.

It is a mild Saturday afternoon at the [Name of Monument / Icon] with a large crowd of visitors on the grounds. The facility employees were briefed to be extra vigilant because of the elevated threat alert issued through NTAS.

A man enters the [Monument / Park / Building] and walks around for a few minutes before he puts his backpack on the ground near [specific incident location] then walks away, leaving the backpack. The backpack is filled with 20lbs of C-4, a common variety of the plastic explosive family, and is activated by a remote device. Approximately 10 minutes later, the IED detonates causing an explosion and mass panic.

In the moments after the explosion, calls flood into 911 from terrified people giving conflicting information about where the explosion came from at [insert monument] and screaming for help for the wounded. Families, separated in the blast and ensuing chaos, are searching for loved ones as calls continue to pour into 911 requesting information. Spectators overwhelm social media with images and live-streamed videos of the attack.

Discussion Questions

1. What steps will your facility take to increase security measures after receiving news of the attack at a National Monuments and Icons facility?
2. What would the protective security posture be at the National Monuments and Icons facility following this domestic attack?
    a. Does your organization coordinate protective measures implementation with any other organizations within the National Monuments and Icons subsector, local or state law enforcement agencies, or your CISA Protective Security Advisors (PSA)?
3. What protocols exist to properly respond to the incident?
    a. How has your organization trained personnel to provide guidance to employees and visitors for this type of incident?
    b. What types of notification systems exist to warn employees both on and off-site?

4. What specific emergency preparedness actions or protective measures would local law enforcement, state, and federal partners take in response to this threat information?
5. What local, state, and federal resources are available to support the National Monuments and Icons facility's response?
    a. What does that coordination with local, state, and federal agencies look like?
    b. What assets or resources are available?
6. How do different agencies and organizations cross-train for this type of incident?
    a. Do local law enforcement and on-site security conduct cross-training?
    b. Does the cross-training address complex coordinated attacks?
7. What type of command structure would responders establish?
    a. Who would be in charge of the command structure?
    b. How would private sector stakeholders integrate into this command structure?
        i. What role would the private sector have?
        ii. Do private stakeholders train on the Incident Command System (ICS) or the National Incident Management System (NIMS)?
8. What mutual aid agreements are in place?
    a. Would emergency declarations impact the availability of resources?
    b. Are there formal agreements that dictate how your organization coordinates with any other sector?
    c. If so, how does your organization activate these agreements, i.e., what type of coordination / information sharing does your organization require?
    d. How does your organization communicate this subsequent information?
9. How would public and private sector stakeholders share information during this incident?
    a. What platforms would public and private stakeholders use to share this information?

b. How would stakeholders share pertinent information with similar facilities, or other monuments and icons to prevent potential future attacks?

10. What key messages do the private and public sector need to communicate to the public?

a. Who is responsible for coordinating the message for the [insert National Monuments and Icons facility]?

b. How do state and local officials coordinate messages?

c. How will your facility and local officials disseminate this public messaging?

Scenario Update
[Insert Location]

[Month, Day, Year]: 1:35 p.m.

Forty-five minutes have passed since the attack at [insert location] and police officials are still attempting to identify the individual who detonated the backpack IED. Incident Command was established and first responders are continuing to treat and transport victims to local hospitals. At this time, all visitors that were [in the building/on the grounds] have been evacuated.

Additional resources have arrived at the scene and secondary sweeps have begun. Law enforcement officers locate a secondary backpack at [insert location] and discover an IED inside.

Discussion Questions

1. At this time, what are the messages your organization is disseminating to the public?
    a. Who is responsible for sharing that message?
2. What information are you sharing with employees?
    a. How does your organization communicate that information?
3. Does your organization have pre-identified Public Information Officers (PIOs)?
    a. If so, what role would the PIOs play in relaying this information to the public?
4. Is someone within your organization monitoring social media to maintain awareness of information spreading that may not be accurate?
    a. Who is responsible for monitoring the spread of inaccurate information on social media?
    b. What procedures exist to counter false information?
5. What mutual aid agreements exist, if any, that your organization could use to assist in response based on the scenario?
6. Which hospitals or health care facilities would your organization expect to receive incident victims?
    a. How are victims identified and tracked within the medical system?
7. What procedures and mutual aid agreements are in place to assist with resource shortages?
8. What role do private and public sector stakeholders play in the established Incident Command structure?

9. Is your organization trained in incident command procedures?

This page is intentionally left blank.

MODULE THREE: SHORT-TERM RECOVERY

Scenario

[Insert Location]

[Insert 48 Hours Later]

Two days have passed, and first responders reported that there are estimates of at least [X fatalities, X critical injuries, and X with minor injuries] resulting directly from the IED attack or the ensuing panic.

The law enforcement investigation continues, and people are still restricted from entering the area around the [National Monument location]. City officials have begun the damage assessment process to determine the facility repair costs.

As expected, social media is rampant with rumors and speculation about the incident. Some claim there were explosive devices placed inside facilities near the [monument], while others claim there were multiple backpacks around the vicinity. Several news outlets continue to dispatch reporters to the scene to interview any remaining witnesses and capture footage of the destruction. The mayor's office is inundated with requests for interviews with employees and local officials.

Additionally, 911 call centers have received numerous requests for information about the incident from families and friends worried about loved ones who may live near the incident site or were visiting [insert city area].

Discussion Questions

1. What communication takes place between organization officials and first responders after the incident?
    a. What other agencies / organizations does your organization need to contact at this time?
2. How does the investigation affect other nearby businesses?
3. Are there sufficient available resources for local response agencies to respond to all incidents, including any day-to-day operational calls?
    a. What additional resources is your organization considering to assist in short-term recovery?
    b. What state and federal resources would your organization request, if any?
4. What contracts exist for debris clean up?

5. Would someone from your organization be responsible for setting up family assistance or reunification centers immediately following the incident?
    a. If so, who is responsible for this?
    b. What procedures are in place for this?
    c. How are families made aware of where to go?
6. What mental health or trauma counseling services does your agency / organization have available for employees?
7. What coordination exists between law enforcement and local hospitals regarding patient tracking?
8. Is someone within your organization monitoring social media to maintain awareness of false information, if any, being spread?
    a. Who is responsible for this?
    b. What procedures are in place to counter false information?
9. Who will the media overwhelm with interview requests?

Scenario Update
[Insert Location]

Date: [Insert One Week Later]

It has been one week since the attack. Internal and external repairs to the damage caused by the backpack IED continue around the [incident location]. At least half of the impacted facilities from the incident still have many employees unavailable for work. The attack has left many employees with psychological and mental trauma, with many expressing an unwillingness or inability to come back to the attack site.

Discussion Questions

1. What is the financial impact on your organization during the time it is closed?
    a. What is the financial impact on the surrounding businesses?
2. What legal impacts would your organization face going forward?
3. At what point would your organization consider the National Monuments and Icons facility and surrounding businesses stabilized and back to steady state?
    a. Who determines when it is safe for employees / visitors to return after such an incident?
    b. How does your organization communicate that message to the public?
    c. How would your organization(s) encourage employees / visitors to return after such an incident?
4. How will your organization(s) begin to return confidence to the American people?
    a. What kind of events or promotional opportunities will your organization use to achieve this goal?
5. Who would coordinate memorials for those who perished during the attack?
    a. Does your state, county, or city have any laws restricting the duration or location of memorials?

This page is intentionally left blank.

APPENDIX A: EXERCISE PARTICIPANTS

Participating Organizations
Private Sector
[Private sector participants]
Local
[Local Participants]
State
[State Participants]
Federal
[Federal participants]
Other
[Insert additional participants]

This page was intentionally left blank.

APPENDIX B: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Term
AAR	After-Action Report
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
DHS	Department of Homeland Security
EMS	Emergency Medical Services
EPT	Exercise Planning Team
FBI	Federal Bureau of Investigation
HSIN	Homeland Security Information Network
ICS	Incident Command System
IED	Improvised Explosive Device
IP	Improvement Plan
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NTAS	National Terrorism Advisory System
PIO	Public Information Officer
POC	Point of Contact
PSA	Protective Security Advisor
SitMan	Situation Manual
SME	Subject Matter Expert
TTX	Tabletop Exercise

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY